Claims

I claim on a:

1. Method and procedure to be used between two remote entities that had for once performed a direct contact, and wishes to authenticate each other's identity afterwards in a repetitive indirect communication between themselves via an unsecured electronic, electromagnetic or sonic media, and:

are using for that purpose a system that is built upon two exact copies of a fixed length line of cells, that exists in parallel in the hands of both entities- one copy per each entity, and:

the order of the cells in the line can be reconfigured, and:

the reconfiguration of the order of the cells, whenever it is performed, is done simultaneously at the same time, and in the same order, in such a manner that the two lines remain identical at all times, and

each cell in the line can be identified by its position in the line, and:

each cell carries in it a code that is replaced every time it has been used in a way that:

both sets must replace the same codes in the same cells in the line at the same time, so that the two sets of codes in the cells of the lines remain identical at all times, and:

the initial loading of the codes is performed in the initial direct contact of the entities, and:

the actions that are preformed on the set, in order to provide the entity authentication include:

an exposure of different cells for each connection, and:

submitting the exposed calls' codes by the authenticating providing side to the authentication requesting side as an authentication prove, while:

the selection of at least one cell that will be exposed is made by a random point out of the authentication asking side, and:

replacing in both copies of the line each code that has been exposed by a newly created code for the next communication, and:

rearranging the order of the cells in both copies of the line for the next communication.

2. Method according to claim 1 wherein the arranging of the cells is in a loop as a ring.

3. Method according to claim 1 wherein instead of arranging the cells in line, they are arranged in more than one dimension grid, so that the position of each cell is determinate by more than one parameter.

4. Method according to claim 1 wherein the codes that have been exposed can be used as a base to create an encrypted communication

5. Method according to claim 1 wherein the authentication is performed by submitting a combination that has been created out of more than one code, in such a way that the original codes can not be recognized in the transition.

6. Method according to claim 4 wherein the combination that has been created out of more than one code can be used as a base to create an encrypted communication.

7. Method according to claim 3 and 5 wherein the authentication is performed by passing only an agreed message, where its correct decryption confirms the identity of the sender.

8. Method to double the strength of any encrypting method by using different codes to separate between the incoming encrypting code and the outgoing encrypting code, in remote encrypted communication.